IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	CRIMINAL NO. 02-118-A
	)	
SABUJ PATTANAYEK,	)	
	)	
Defendant.	)	

STATEMENT OF FACTS

Were the United States to proceed to trial in this case, it would provide testimonial and documentary evidence to prove beyond a reasonable doubt that from at least November 2000 through December 11, 2001, defendant Sabuj Pattanayek (hereinafter "the Defendant"), was knowingly part of a criminal conspiracy to illegally reproduce and distribute copyrighted software, computer games and movies, on a worldwide basis, via the Internet, in violation of federal criminal copyright laws, 17 U.S.C. §506(a) and 18 U.S.C. §2319. Specifically, the testimonial and documentary evidence would establish, at a minimum, the following facts:

The Defendant's willful conduct included his participation in the so-called "warez scene,"[1] and in particular his

[1]"Warez" and "pirated software" are terms used to describe digital copies/reproductions of copyright-protected computer software, games, movies, and music that are distributed and traded over the Internet in violation of copyright law. The "warez scene" refers to the complex web of both informal and formal Internet communication, distribution and trading channels used by individuals that engage in

participation in the warez "release" group DrinkOrDie (DOD) and the warez courier group Return To Sender (RTS). DOD was a highly structured criminal organization that specialized in distributing (or releasing) "cracked"[2] copyrighted computer software over the Internet. The group sought to achieve a reputation as the fastest provider of the highest quality application and utility software (e.g., Symantec security software, Microsoft and AutoDesk applications) to the warez scene. RTS is a so-called "courier" group that specializes in moving, or transferring, new warez releases (e.g., software, games, movies) from one warez Internet site to another.

Defendant knew that his participation in DOD and RTS was illegal, and he was aware of past federal prosecutions against similar groups. All warez activities were conducted in a highly security conscious environment with an emphasis on secrecy. For instance, all DOD group business was discussed in closed, invite-only Internet Relay Chat (IRC) channels, and staff members encrypted e-mails to each other, using the group's private electronic mailserver, when communicating about group business. Members were never identified by their real names, only by their

---

this form of software piracy.

[2]As used here, "cracked" means that the software's copyright protections are removed or circumvented.

screen nicknames. The Defendant, for instance, was known online only by the moniker "buj."

Rank and position in DOD was based on a variety of factors, including special skills, length and quality of service to the group, and reputation within the warez scene. DOD had two co-leaders, 2-3 council, 12-15 staff, and a general membership comprising approximately 65 individuals. The two co-leaders had ultimate authority over all aspects of the group; council members assumed primary responsibility for the group's day-to-day operations, including preparation of new releases, recruitment, and security issues; staff were generally the members who were most active in preparing the group's new releases for distribution, or in maintaining the group's FTP sites; and general members contributed to the group in a variety of ways, including acting as occasional suppliers of new software, hosting the group's FTP servers and bounce boxes, or providing hardware (e.g., laptops, hard drives, routers, other computer equipment) to other group members for use in their warez activities.

From November 2000 through December 11, 2001, Defendant was first a staff member, and later a council member, in DOD. A majority of his contributions to DOD were made as a staff member. He was especially skilled in "cracking," that is, defeating or circumventing copyright protections embedded in software

programs, and he participated in virtually every aspect of the group's "release" work.

DOD's "release" work involved a multi-staged process by which the group acquired, cracked, and distributed (i.e., released) copyrighted software over the Internet. Members known as "suppliers," provided new software to the group in digital format (i.e., the ISO version), sometimes days or weeks before the manufacturer's public release date. Once the supplier posted the product to the group's "drop site,"[3] other group members known as "crackers," applied their special programming skills to defeat the software's embedded copyright protections (e.g., license keys, anti-duplication and dongle security mechanisms), if necessary. After the software had been cracked, it was quality tested and "packed" into data files that could be more easily distributed over the Internet. Finally, group members known as "pre-ers" prepared the final warez product for release and quickly distributed it to a select group of warez FTP[4] sites

[3] A "drop site" is simply a computer site on the Internet that serves as a work station and initial distribution point for the group's warez release work. It may also serve as an archive for the group's warez releases. Access to the site is strictly controlled by a combination of security measures, including password protection and user and IP address verification.

[4] "FTP" stands for File Transfer Protocol, a communication protocol for transferring files between computers connected to the Internet.

worldwide (aka "0-Day Sites"[5]). From these sites, the warez software would be further distributed by courier groups to an ever-expanding web of FTP sites. Within hours, the new release could be on hundreds of warez FTP sites throughout the world. In each instance, the new warez product contained an embedded ".nfo" file that attributed credit for the release to DOD.

Defendant was also an authorized user on a number of FTP "leach" sites controlled by DOD for the benefit of DOD members and warez contributors, including the warez FTP sites known as Fatal Error (applications, games, and movies), Packet Storm (applications archive), Lake of Fire (music), High Octane (mixed), and RatzHole (0-Day). To become an authorized user on one of DOD's FTP sites, a member would need to obtain a password and the domain name for the site's "bounce box"[6] from a site

---

[5]A "0-Day site" is a warez FTP site, connected full-time to the Internet, that receives computer software, game, or movie warez releases on the same day that the originating group releases them to the warez scene.

[6]A "bounce box," as used here, refers to a computer connected full-time to the Internet that contains security and routing software designed to authenticate users and re-route the user to another computer site with a different IP address. The bounce box provides security for warez FTP sites: a user wishing to access the warez site to download or upload pirated software is only given the domain name or IP address for the site's "bounce box." The bounce box contains security software that authenticates the user and automatically re-routes him or her -- once past the security wall -- to the actual warez "leach site" located elsewhere on the Internet. The "leach site" is assigned a different IP address than the bounce box. The user may never know that he has been re-routed to another IP address, and he may never learn the true IP address and location of the "leach site" itself.

In addition, however, the term "bounce box" may be used to

operator, or "site op" who generally was a member of the group's leadership. The member would, in turn, provide the site op with a static IP address, or a narrow range of IP addresses, from which he would access the site. The site op would then configure the bounce box and associated FTP site so that when a member attempted to access the FTP site through the bounce, security software verified his screen nickname, password, and originating IP address before re-routing him to the true IP address of the desired FTP site itself.

Although Defendant did not engage in the commercial sale of pirated software, he did receive "personal financial gain" within the meaning of the criminal copyright statute, see 17 U.S.C. §§101 & 506(a)(1) and the Federal Sentencing Guidelines §2B5.3, Application Note 1, in that he received, and expected to receive, access to other copyrighted works at no cost.

Defendant acknowledges that, through the aforementioned acts and others, he did willfully enter into an agreement with one or

---

reference a computer connected full-time to the Internet which acts as a "virtual host" for a user wishing to disguise, or mask, his true IP address in IRC channels. Normally, when a user logs on to an IRC channel to engage in real-time, online discussions with others, the IRC channel records and displays to others in the channel the screen name and IP address of the user. When an IRC user routes through a "virtual host" box before logging on to the desired IRC channel, the IP address that appears in the IRC channel for the user is the IP address (or domain name) of the bounce box, not the user's computer. Defendant and other DOD members routinely used "virtual hosts" to disguise their true IP addresses when communicating in IRC channels, including the invite-only DOD efnet channels #*fatalerror* and #*drinkordie*.

more individuals for the express purpose of unlawfully reproducing and distributing copyrighted materials via the Internet. The defendant also acknowledges that he did so knowing of the unlawful nature of the activity, and through the aforementioned acts and others, acted in furtherance of such agreement in an effort to carry out or accomplish the object of the conspiracy. Defendant also acknowledges that, both individually and through the acts of others in the conspiracy for which he is accountable, he caused the reproduction and distribution over the Internet of more than 10 copies of copyrighted works within a 180-day period having a total retail value of more than $2,500. The Defendant and government agree that, based on the evidence now known to the government, the infringement amount under the provisions of §2B5.3.(b)(1) of the Federal Sentencing Guidelines attributable to the Defendant is more than $2.5 million but less than $5 million.

Respectfully Submitted,

Paul J. McNulty
United States Attorney

By: _____
Robert W. Wiechering
Assistant United States Attorney

By: _____
Michael M. DuBose, Senior Counsel

Computer Crime & Intellectual
Property Section
Department of Justice

Seen and Agreed:

_____
Sabuj Pattanayek
Defendant

_____
Joseph H. Craven, Esq.
Counsel for Defendant